UJI KEAMANAN KOMUNIKASI VOIP MENGGUNAKAN SISTEM KEAMANAN SRTP-TLS PADA JARINGAN NIRKABEL

Tri Febriana Handayani[1], Pande Ketut Sudiarta[2], I Made Oka Widyantara[3]
[123]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Udayana
Email : Febrianahandayani12@gmail.com[1] , Sudiarta@unud.ac.id[2], Oka.widyantara@unud.ac.id[3]

ABSTRAK

VoIP merupakan suatu teknologi yang digunakan untuk berkomunikasi suara jarak jauh secara langsung dengan menggunakan jalur komunikasi data menggunakan protocol TCP/IP. Namun pada dasarnya komunikasi VoIP tidak menjamin keamanan data saat melakukan komunikasi. Sistem keamanan sangat penting ditambahkan dalam komunikasi VoIP untuk menjaga kerahasiaan komunikasi, sehingga komunikasi yang dilakukan tidak bisa direkam dan diputar ulang. Untuk membangun sebuah keamanan saat berkomunikasi VoIP,maka pada penelitian ini ditambahkan sebuah sistem keamanan SRTP-TLS. Penelitian ini dilakukan pada jaringan nirkabel dengan membandingkan keamanan data komunikasi saat menggunakan sistem keamanan SRTP-TLS dan tanpa menggunakan sistem keamanan.
***Kata Kunci**: Nirkabel, Sistem Keamanan,VoIP*

ABSTRACT

VoIP is a technology used to communicate voice remotely and directly using data communication lines with TCP / IP protocol. But basically, VoIP communication does not guarantee data security when doing communication. A very important security system is added in VoIP communications to maintain the confidentiality of communication, so that communication can not be recorded and played back. To build a security when communicating VoIP, then in this study added an SRTP-TLS security system. The study was conducted on wireless networks by comparing the security of data communications when using the SRTP-TLS security system and without using a security system.
***Keywords**: Wireless, Security System, VoIP*

1. PENDAHULUAN

VoIP ialah teknologi yang dapat melewatkan data suara, video dan data yang berbentuk paket memakai jaringan IP. Jaringan IP merupakan jaringan komunikasi data (*packet-switch*), jadi dalam berkomunikasi memanfaatkan jaringan IP atau Internet. VoIP menjadi media untuk berkomunikasi, tetapi dalam suatu jaringan. *Voice* dari *user* akan diubah dalam bentuk digital dan dikirimkan bentuk paket data secara *real time* [1]. Jaringan yang dimanfaatkan berupa *internet* atau *intranet*. Sinyal suara analog. Dengan berkomunikasi menggunakan layanan VoIP, banyak keuntungan yang didapatkan, salah satu keuntungannya yaitu konsumsi biaya yang lebih sedikit untuk sambungan langsung jarak jauh (SLJJ). [2] Karena penggunaan jalur internet, biaya hanya pada biaya internet. Dengan dua lokasi yang sudah dihubungkan internet, maka biaya percakapan menjadi sangat rendah [3].

Dengan terbukanya sistem komunikasi VoIP mengakibatkan semua orang mampu mempelajari, menyadap dan mengembangkan VoIP. Dalam pengoperasiannya, layanan VoIP tidak menjamin keamanan data paket pada setiap komunikasi suara. Hal ini memungkinkan dilakukannya aksi penyadapan pada isi komunikasi VoIP [4]. Untuk mengatasi kerentanan ini, maka salah satu solusinya adalah dengan mengimplementasi sistem keamanan pada komunikasi VoIP. Sistem keamanan yang dapat digunakan adalah *Secure Real Time Transport Protocol* (SRTP-TLS).

2. KAJIAN PUSTAKA

Teori-teori penunjang yang digunakan dalam penelitian ini adalah sebagai berikut.

2.1 VoIP (*Voice Over Internet Protocol*)

Gambar 1 Diagram VoIP[6]

VoIP ialah teknologi yang dapat melewatkan data suara, video dan data yang berbentuk paket memakai jaringan IP [7]. Jaringan IP merupakan jaringan komunikasi data (*packet-switch*), jadi dalam berkomunikasi memanfaatkan jaringan IP atau Internet [6]. VoIP menggunakan layanan internet untuk berkomunikasi seperti menggunakan telepon pada umumnya dengan pengguna VoIP dimana dan kapan saja. Teknologi layanan komunikasi VoIP mampu melakukan percakapan telepon dengan jalur komunikasi data dalam jaringan (*networking).*

Prinsip kerja dari layanan komunikasi VoIP yaitu mengubah suara masukan berbentuk analog yang didapatkan dari mikropon pada PC atau *softphone* menjadi sebuah paket data berbentuk digital, kemudian dari PC atau *softphone* dilewatkan melintasi *router*, dan dikiriman menggunakan sebuha jaringan internet yag kemudian diterima oleh *user* lain sebagai tempat tujuan melalui media yang sama. Prinsip kerja VoIP digambarkan pada Gambar 1.

Kualitas suara dari layanan komunikasi VoIP tidak jauh berbeda dengan telepon konvensional lainnya, namun kualitas tetap bergantung pada kualitas jaringan telekomunikasi yang sedang digunakan. VoIP mampu diuraikan dengan sederhana sebagai salah satu komunikasi yang memanfaatkan teknologi dengan mengubah suara menjadi bentuk sinyal digital untuk kemudian dikorempresi di beberapa bagian, tanpa harus mengurangi isi dari informasi. *Payload* ini akan dibagi menjadi paket-paket *Internet Protocol* (IP) yang selanjutnya ditransmisikan melalui jaringan *internet*, lalu proses sebaliknya dilakukan di sisi *user* penerima [8].

2.2 *Secure Real Time Transport Protocol* (SRTP)

Secure Real Time Transport Protocol (SRTP) merupakan protokol standar yang digunakan untuk *profile* dari *Real Time Protocol (*RTP). Protokol ini merupakan penyedia autentikasi pesan enkripsi, dan integritas data bagi data RTP. SRTP menyediakan layanan *encryption* pada RTP yang bertujuan memberikan sistem keamanan data dengan autentikasi pesan enkripsi dan integritas data, serta perlindungan terhadap *playback* dengan data RTP. Pengembangan SRTP memanfaatkan algoritma *Advanced Encryption Standart* (AES) sebagai metode enkripsi untuk transmisi data. Pengimplementasian SRTP memiliki 2 mode, yaitu *Segmented Integer Counter*, dan AES. SRTP juga dapat diimplementasikan pada *mode null cipher*, mode *null cipher* adalah sebuah mode pengiriman data yang tidak terlindungi algoritma enkripsi. Pada kenyataannya SRTP hanya mengenkripsi *payload* (*audio* dan video) untuk kerahasiaan. SRTP pada komunikasi VoIP memiliki fungsi untuk mengenkripsi komunikasi data VoIP. Hal ini bertujuan untuk memastikan jaminan aspek *privacy* dan *integrity*. SRTP merupakan algoritma enkripsi yang dimanfaatkan khusus sebagai komunikasi VoIP. SRTP digunakan sebagai enkripsi *media stream* yang mengakibatkan *payload* gagal dibaca saat terjadi trafik *capturing*. Pada SRTP terjadi autentikasi pengiriman untuk mengantisipasi penyadapan identitas namun validasi *integrity* digunakan untuk mengantisipasi modifikasi pesan yang dikirimkan [4].

Cara kerja SRTP sama dengan RTP, yaitu dengan mendukung dan mengupayakan komunikasi VoIP dapat berjalan secara *real-time*. Namun, pada *format* protokol SRTP ditambahkan SRTP *message* untuk memberikan fasilitas

enkripsi. Sebelum membangun komunikasi VoIP, dilakukan pertukaran kunci master terlebih dahulu antar dua *client* yang berkomunikasi. Kunci master dapat dibangun menjadi dua kunci sesi, diantaranya kunci sesi enkripsi dan kunci sesi autentikasi. Kunci enkripsi digunakan untuk mengenkripsi data VoIP sehingga informasi tidak didapatkan secara langsung atau tidak berupa *plaintext*. Sedangkan kunci autentikasi berfungsi sebagai validasi data dan menjamin penerima adalah tujuan yang benar. Hal ini bertujuan untuk mencegah pemalsuan identitas. Setelah terjadi pertukaran kunci, kunci-kunci tersebut akan digunakan untuk mengenkripsi data sebelum dikirimkan. Pada waktu tertentu kunci sesi ini akan berubah-ubah secara *random* [5].

2.3 *Transport Layer Security* (TLS)

Transport Layer Security (TLS) dan *Secure Socket Layer* (SSL) adalah protokol *cryptographic* berfungsi untuk mengamankan komunikasi di internet (*web browsing*, *email*, *internet facing,* dan *instant messaging)*. Aplikasi dapat berkomunikasi untuk melewati jaringan lain dengan TLS guna mencegah aktifitas penyadapan (*eavesdropping*), perusakan (*tampering*) dan pemalsuan pesan (*message forgery*). *Authentication end point* dan keleluasaan komunikasi pribadi pada jaringan *internet* dengan menggunakan *cryptography* disediakan oleh TLS (*Transport Layer Security*) [9].

authentikasi pengirim dan penerima yang telah terdeteksi oleh *server* (kepastian pengenalan) disebut juga sebagai *authentication* timbal balik. *Authentication* ini membutuhkan *public key infrastructure* (PKI) yang menyebar ke klien, kecuali pada TLS-PSK atau protokol *Secure Remote Password* (SRP) digunakan sebagai penyedia *authentication* timbal balik yang kuat tanpa perlu mengirimkan PKI. TLS menggunakan tiga tahap dasar yaitu [10]:

1. *Peer* negosiasi untuk *support* algoritma
2. Penukaran kunci dan *authentication*
3. Enkripsi kode *symmetric* dan perlu pesan *authentication*

Klien TLS dan *server* bernegosiasi dengan menggunakan prosedur *handshaking*. Berbagai parameter yang digunakan untuk tetap berkoneksi disetujui klien dan *server* pada saat proses *handshake*. Proses *handshake* dapat dijabarkan sebagai berikut.

1. *Handshake* terjadi saat klien meminta *server* TLS mengamankan koneksi dan menampilkan *ciphers* (berupa bilangan biner/bahasa mesin) dan *hash function*.
2. Dari daftar ini, *server* meminta kembali *chipher* (berupa bilangan biner/bahasa mesin) dan *hash function* kemudian memberitahukan keputusannya kepada klien.
3. Identifikasinya dalam bentuk sertifikat digital yang berisi *authory* dan enkripsi kunci *server public* dikembalikan oleh *server*.

Klien diizinkan menghubungi *server* untuk meyakinkan sertifikat asli sebelum melanjutkannya kembali. Enkripsi klien diacak dengan kunci *public* untuk menghasilkan kunci enkripsi dan deskripsi di kedua belah pihak. Ini mengakibatkan proses *handshake*, awal koneksi, dan akhir koneksi terjamin keamanannya. Jika langkah-langkah tersebut gagal, *handshake* TLS gagal maka koneksi tidak dapat dibangun.

2.4 *Softphone*

Selain dalam bentuk *hardware*, perangkat telepon juga bisa berbentuk *software*. Contoh *software* yang digunakan untuk komunikasi VoIP adalah *softphone*. *Softphone* adalah aplikasi *client* VoIP yang dapat mendigitalisasi data suara dalam bentuk paket data untuk ditransmisikan melalui jaringan. Pesan yang ditransmisikan dapat berupa *voice* maupun video.

2.5 FreePBX

FreePBX merupakan aplikasi untuk pengontrolan jaringan IP telepon yang mengkonfigurasi *web GUI*, sehingga lebih mudah untuk mengkonfigurasi Asterisk.

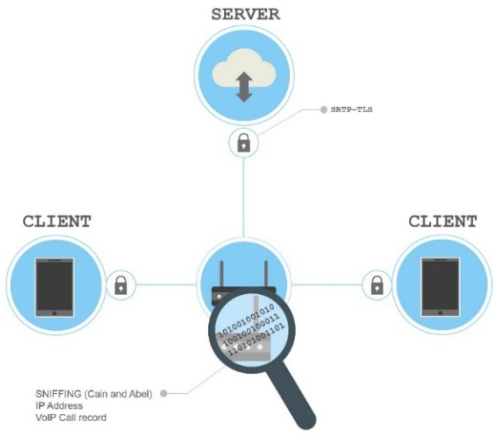
2.6 Cain and Abel

Sniffer atau *network analyzer* merupakan *software* atau *hardware* yang berfungsi untuk menghalangi dan mencatat semua trafik sebuah jaringan. *Sniffer* juga berfungsi untuk menangkap seluruh trafik paket data pada jaringan. Pada penelitian

ini *sniffer* yang digunakan adalah Cain and Abel.

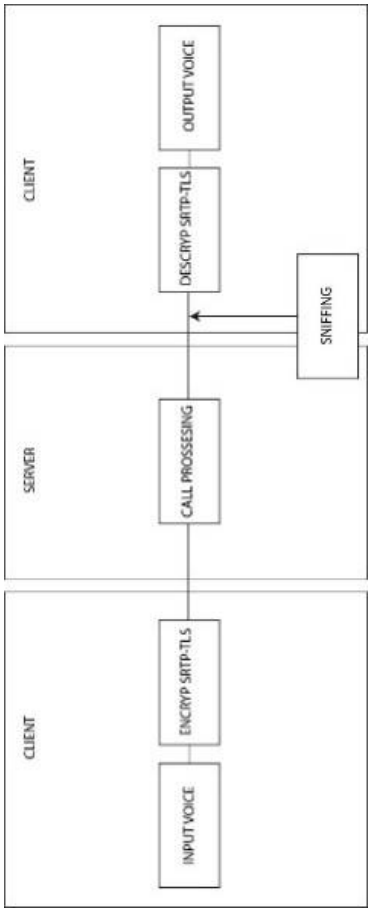
3. METODOLOGI PENELITIAN

Skenario penelitian digambarkan pada Gambar 2. Pada Gambar 2, terlihat bahwa ada 2 buah klien dengan masing-masing klien menggunakan PC yang sudah ter-*install softphone* sebagai *software* untuk komunikasi suara. *Codec* yang digunakan masing-masing klien adalah G. 711. Layanan VoIP disediakan oleh *server* VoIP yaitu FreePBX. Agar pengujian keamanan dapat dilakukan, maka pada jaringan sistem ini dipasang sebuah aplikasi yang dapat melakukan penyadapan terhadap komunikasi yang dilaukan berupa *software* Cain and Abel.



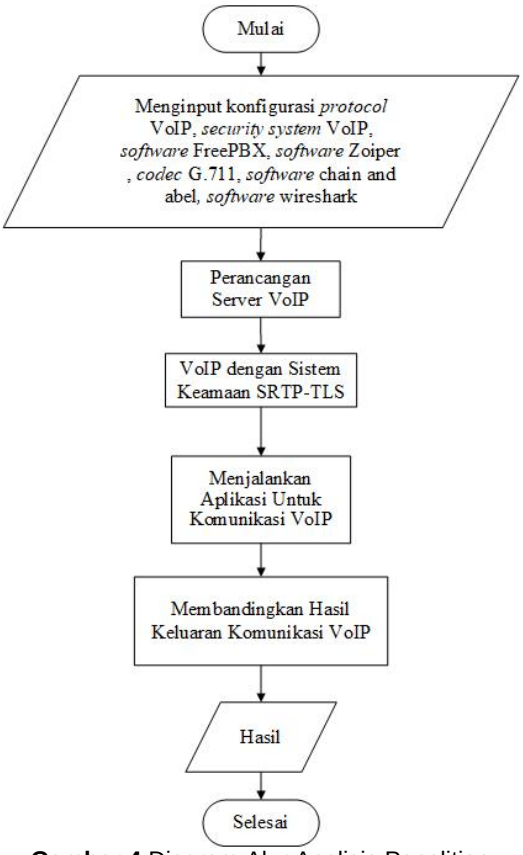
Gambar 2 Diagram Skenario Penelitian

Proses *Sniffing* dimulai dengan meng-*input voice* melalui *microphone*. Pada perangkat suara atau *voice* akan langsung mengalami proses enkripsi (SRTP-TLS). Seluruh proses ini terjadi pada sisi *client* hingga ditranmisikan ke sisi *server*. Pada sisi *server,* data *voice* yang telah dienkripsi akan ditransmisikan (*Call Prossesing*) kembali ke sisi *client* tujuan (IP tujuan). Sebelum *voice* menjadi *output* oleh *microphone*, data akan mengalami proses deskripsi agar data sesuai dengan data awal sebelum dienkripsi. Proses *sniffing* dapat terjadi pada jalur IP sumber ataupun IP tujuan. Dengan proses *sniffing* akan didapatkan rekaman suara yang masih terenkripsi. Blok diagram proses *sniffing* tersebut digambarkan pada Gambar 3.



Gambar 3 Blok Diagram Proses Sniffing

Faktor yang menentukan keamanan pada sebuah komunikasi menggunakan SRTP-TLS adalah dapat atau tidaknya sebuah percakapan direkam dan diputar kembali.



Gambar 4 Diagram Alur Analisis Penelitian Dengan SRTP-TLS

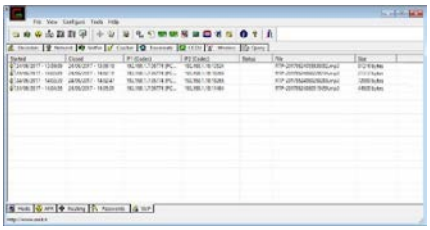
Gambar 4 merupakan alur analisis. Sistem dimulai dengan memberikan *input*an konfigurasi iprotocol VoIP, *security system* VoIP, *software*, FreePBX, *software* Cain and Abel. Kemudian melakukan perancangan pada *software* FreePBX sebagai *server* VoIP dengan mengimplementasikan sistem keamanan SRTP-TLS dan menggunakan *codec* G7.11. jika *server* VoIP telah menggunakan sistem keamanan SRTP-TLS, maka sebuah komunikasi VoIP dengan sistem keamanan SRTP-TLS akan terbentuk. Analisis dilakukan dengan cara membandingkan keluarkan komunikasi VoIP berupa data *voice* menggunakan *software* Cain and Abel. Jika *server* VoIP tidak menggunakan sistem keamanan SRTP-TLS, maka sebuah komunikasi tanpa sistem keamanan akan terbentuk. Yang kemudian hasil masing-masing keluaran data *voice* pada komunikasi VoIP dengan sistem keamanan SRTP-TLS dengan tanpa sistem keamanan akan dibandingkan, apakah hasil keluaran data *voice* dapat direkam dan diputar kembali. Kemudian sistem akan mengakhiri proses.

4. HASIL DAN PEMBAHASAN

Hasil dan pembahasan pada penelitian ini akan dijabarkan sebagai berikut.

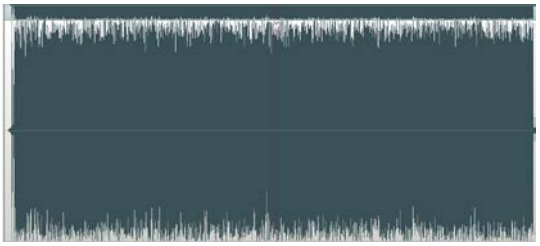
4.1 Pengujian Keamanan SRTP-TLS Pada Jaringan Nirkabel

Pada pengujian yang dilakukan menggunakan sistem keamanan SRTP-TLS pada jaringan nirkabel, komunikasi dapat direkam namun hasil rekam yang didapatkan hanya menampilkan suara *noise*. Hal tersebut terjadi karena sistem keamanan SRTP yang sudah diimplementasikan pada komunikasi yang sedang dibangun mengenkripsi *payload*. SRTP memiliki fitur enkripsi pada profil RTP yang berfungsi untuk menyediakan sistem keamanan data dengan autentikasi dan integritas pesan, dan perlindungan terhadap *playback* (diputar kembali). Kemungkinkan klien untuk mengautentikasi *server* dan opsional *server* untuk mengautentikasi klien dienkripsi oleh TLS.



Gambar 5 Hasil Rekaman Komunikasi pada Cain and Abel

Gambar 5 merupakan beberapa hasil rekaman komunikasi yang menggunakan sistem keamanan SRTP-TLS, dan ditampilkan dalam *software* Cain and Abel.

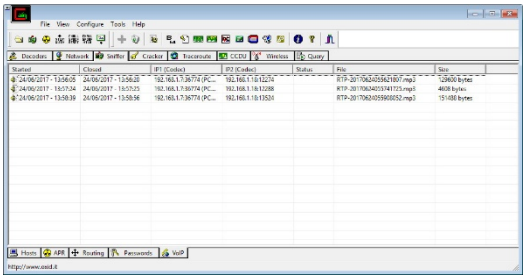


Gambar 6 Tampilan hasil rekam *voice* SRTP-TLS

Gambar 6 merupakan spektrum suara hasil rekaman komunikasi yang menggunakan sistem keamanan SRTP-TLS. Terlihat spektrum suara tidak berada di garis tengah, dan jika diputar kembali, suara yang dihasilkan hanya *noise.*

Pada pengujian *sniffing* menggunakan Cain and Abel didapatkan hasil bahwa komunikasi VoIP dapat dilakukan.

4.2 Pengujian Keamanan TLS Pada Jaringan Nirkabel



Gambar 7 Hasil Rekaman Komunikasi pada Cain and Abel

Gambar 7 merupakan beberapa hasil rekaman komunikasi yang menggunakan sistem keamanan TLS, dan ditampilkan dalam *software* Cain and Abel.

Gambar 8 Tampilan hasil rekam *voice* TLS

Gambar 8 merupakan spektrum suara hasil rekaman komunikasi yang menggunakan sistem keamanan TLS. Terlihat spektrum suara berada di garis tengah, dan jika diputar kembali, suara yang dihasilkan adalah suara ketika komunikasi berlangsung.

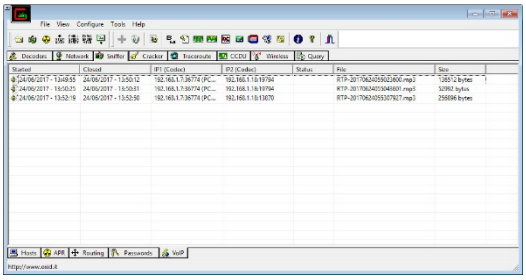
Pada pengujian *sniffing* menggunakan Cain and Abel didapatkan hasil bahwa komunikasi VoIP dapat dilakukan namun membutuhkan waktu yang lebih lama untuk pembangunan komunikasi dikarenakan prosedur *handshaking* yang harus menyetujui berbagai parameter yang digunakan untuk membangun komunikasi, pada pengujian yang dilakukan menggunakan sistem keamanan TLS bisa direkam dan diputar kembali, namun kualitas suara rekaman tidak baik, ini dikarenakan pengaruh dari jaringan nirkabel yang digunakan. Karena jaringan nirkabel mempunyai sifat yang fluktuatif atau tidak stabil. Jika pada saat melakukan komunikasi jaringan yang digunakan baik, maka kualitas suara yang dihasilkan relatif baik, dan begitu sebaliknya.

Hal tersebut terjadi karena sistem keamanan TLS merupakan protokol yang menyediakan komunikasi privasi dan keamanan antara dua aplikasi berkomunikasi melalui jaringan. Sesuai dengan penjabaran sistem keamanan TLS yaitu mengenkripsi komunikasi dan memungkinkan klien untuk mengotentikasi *server* dan opsional *server* untuk mengotentikasi klien.

4.3 Pengujian Tanpa Sistem Keamanan Pada Jaringan Nirkabel

Pada komunikasi VoIP yang dilakukan tanpa menggunakan sistem keamanan, didapatkan hasil komunikasi VoIP bisa melakukan panggilan yang juga dapat di rekam tanpa adanya masalah. Karena komunikasi VoIP yang dilakukan pada pengujian ini tanpa menggunakan sistem keamanan, maka seluruh komunikasi dapat di-*sniffing* menggunakan Cain and Abel.

Hasil *sniffing* tersebut berupa sebuah rekaman komunikasi dan dapat diputar dengan baik. Pengujian tanpa sistem keamanan yang dilakukan sesuai dengan latar belakang pada penelitian ini yaitu dalam pengoperasiannya, layanan komunikasi VoIP tidak menjamin keamanan data paket setiap dilakukannya sebuah komunikasi.



Gambar 9 Hasil Rekaman Komunikasi pada Cain and Abel

Gambar 9 merupakan beberapa hasil rekaman komunikasi tanpa menggunakan sistem keamanan dan ditampilkan dalam *software* Cain and Abel.

Gambar 10 Hasil rekam *voice* tanpa sistem keamanan

Gambar 10 merupakan spektrum suara hasil rekaman komunikasi tanpa menggunakan sistem keamanan. Terlihat spektrum suara berada di garis tengah, dan jika diputar kembali, suara yang dihasilkan adalah suara ketika komunikasi berlangsung.

Dari masing-masing pengujian menggunakan 3 kondisi, yaitu: pengujian dengan sistem keamanan SRTP-TLS, pengujian dengan sistem keamanan TLS, pengujian tanpa sistem keamanan, didapatkan hasil sebagai berikut:

Tabel 1 Hasil Seluruh Pengujian Keamanan Menggunakan Jaringan Nirkabel

Pengujian	Hasil
Sistem keamanan SRTP-TLS	Komunikasi bisa direkam, namun tidak bisa diputar kembali (berbentuk *noise)*
Sistem keamanan TLS	Komunikasi bisa direkam dan bisa di-putar kembali
Tanpa sistem keamanan	Komunikasi bisa direkam dan bisa di-putar kembali

Pada pengujian yang dilakukan menggunakan sistem keamanan SRTP-TLS, komunikasi dapat direkam namun hasil rekam yang didapatkan hanya menampilkan suara *noise*. Hal tersebut terjadi karena sistem keamanan SRTP yang sudah diimplementasikan pada komunikasi yang sedang dibangun mengenkripsi *payload* untuk kerahasiaan. Sedangkan TLS mengenkripsi komunikasi dan memungkinkan klien untuk mengautentikasi *server*.

Pada komunikasi VoIP yang dilakukan menggunakan jaringan nirkabel dengan sistem keamanan TLS didapatkan hasil bahwa komunikasi VoIP dapat dilakukan namun membutuhkan waktu yang lebih lama untuk pembangunan komunikasi dikarenakan prosedur *handshaking* yang harus menyetujui berbagai parameter yang digunakan untuk membangun komunikasi. Pada pengujian yang dilakukan menggunakan sistem keamanan TLS bisa direkam dan diputar kembali, namun kualitas suara rekaman tidak baik, ini dikarenakan pengaruh dari jaringan nirkabel yang digunakan. Karena jaringan nirkabel mempunyai sifat yang fluktuatif atau tidak stabil. Jika pada saat melakukan komunikasi jaringan yang digunakan baik, maka kualitas suara yang dihasilkan relatif baik, dan begitu sebaliknya.

Sedangkan pada komunikasi VoIP menggunakan jaringan nirkabel yang dilakukan tanpa menggunakan sistem keamanan, didapatkan hasil komunikasi VoIP bisa melakukan panggilan yang juga dapat di rekam tanpa adanya masalah. Karena komunikasi VoIP yang dilakukan pada pengujian ini tanpa menggunakan sistem keamanan, maka seluruh komunikasi dapat di-*sniffing* berupa sebuah rekaman komunikasi dan dapat diputar dengan baik.

5. KESIMPULAN

Penambahan sistem keamanan SRTP-TLS pada komunikasi VoIP di jaringan nirkabel terbukti aman. Keamanan tersebut dapat dibuktikan dari komunikasi yang dilakukan saat menggunakan sistem keamanan SRTP-TLS, tidak dapat direkam dan diputar ulang. Berbeda halnya jika

tidak menggunakan sistem keamanan dan hanya menggunakan sistem keamanan TLS, komunikasi VoIP yang dilakukan bisa direkam dan diputar ulang dengan mudahnya. Beberapa kualitas komunikasi yang tidak baik, dipengaruhi oleh jaringan nirkabel yang digunakan mempunyai sifat yang fluktuatif atau tidak stabil.

Untuk pengembangan penelitian ini, maka dapat dilakukan dengan mengujicobakan *codec* dan protocol VoIP yang berbeda, serta dengan perbandingan jarak.

6. DAFTAR PUSTAKA

[1] Irwansyah, E. & Jurike V, M,. 2014. "Pengantar Teknologi Informasi," Yogyakarta : *Deepublish*. 2014.

[2] Zaki, A. "Berkomunikasi Murah Via Internet". *Elex Media Komputindo*. 2008

[3] Zaki, A. SmitDev Community. "Berkomunikasi Murah Via Internet." *Elex Media Komputindo*. 2008

[4] Kurniawan, FM. 2014. "Implementasi SRTP-TLS Pada VoIP" Diakses pada 6 Desember 2016. <ilmukomputer.com>

[5] Kalwar, S, K. Khan, M. "SECURED REAL TIME TRANSPORT PROTOCOL (SRTP)". *Lappeenrannan University Of Technology, Department Of Information Technolog.* 2007

[6] Tharom, T. "Teknis dan Bisnis VoIP". Jakarta : *PT. Elex Media Komputindo*. 2002

[7] Iskandarsyah, M. "Cara Mudah Membangun Jaringan VoIP". *Bandung : Kawan Pustaka*. 2003

[8] Astriani, Dwiarum. 2013. "Teknologi VoIP". Diakses Juli 2017. <http://ilmukomputer.org/2013/01/31/teknologi-voip/>.

[9] Bilien, J. et al. "Secure VoIP: Call Establishment and Media Protection". *Royal Institute of Technology (KTH). Stockholm, Sweden*. 2004

[10] Ariyus, Dony. " KRIPTOGRAFI Keamanan Data dan Komunikasi". *Graha Ilmu*. 2006